Electronic Version
Stylesheet Version v1.1.1

A method for dense and secure transmission of signals and information using a small number of channels

Abstract

Suppose that there are n Senders and r Receivers. Our goal is to design a communication network such that long messages can be sent from Sender i to Receiver p(i) such that no other receiver can retrieve the message intended for Receiver p(i). The task can easily be completed using some classical interconnection network and routers in the network. Alternatively, if every Receiver is directly connected to all n Senders, then the Senders can choose which channel to use for communication, without using any routers. Fast optical networks are slowed down considerably if routers are inserted in their nodes. Moreover, handling queues or buffers at the routers is extremely hard in all-optical setting. An obvious routerless solution, connecting each possible Sender-Receiver pairs with direct channels seems to be infeasible in most cases. A method, solving this problem, is disclosed in which the Senders and the Receivers are connected with only a small number of channels (in practice no more than 32 channels); there are no

switching or routing-elements in the network, just linear combinations of the signals are computed. Such designs are usable in fast all-optical networks. The security of the network does not depend on any unproven cryptographical or complexity theoretical assumptions.